АННОТАЦИЯ

В работе рассматривается применение методов цифровой криминалистики в инженерной практике телекоммуникаций и связи. Цифровая криминалистика представлена не как юридическая процедура, а как аналитический инструмент, позволяющий инженеру выявлять источники угроз, локализовать инциденты в высоконагруженных сетях и предотвращать повторные отказы инфраструктуры.

Особое внимание уделено специфике анализа цифровых следов в телеком-системах: сетевому трафику (от BGP до SIP), дампированию оперативной памяти, анализу прошивок встроенных устройств и работе с журналами аутентификации на сетевом оборудовании. В работе показано, как методы криминалистики трансформируются в инструменты глубокой инженерной диагностики.

Целью работы является формирование системного мышления при анализе инцидентов. Задачи включают: изучение природы цифровых следов в инфраструктуре связи; освоение методов фиксации состояния систем (включая тактику Triage); анализ трафика и журналов событий; оценку рисков, связанных с прошивками (Firmware), и использование ИИ как вспомогательного средства анализа.

Работа носит учебно-аналитический характер и ориентирована на студентов и специалистов инженерных направлений.

ВВЕДЕНИЕ

Современные телекоммуникационные системы — это сложные распределённые инфраструктуры, где аппаратные средства и программные компоненты работают в режиме реального времени. В процессе эксплуатации инженер связи сталкивается не просто с ошибками, а с каскадными сбоями, вызванными конфигурационными коллизиями, внешними атаками или деградацией оборудования. В этих условиях традиционный подход «устранить последствия и забыть» ведет к накоплению технических долгов и повторным инцидентам.

Инженерное применение цифровой криминалистики — это переход от симптоматического лечения системы к патологоанатомическому исследованию причин. В отличие от юридического подхода, здесь первична не доказательная база для суда, а восстановление цепочки событий (Root Cause Analysis). Такой подход позволяет рассматривать сеть как динамический процесс, оставляющий измеримые и воспроизводимые следы.

Актуальность работы обусловлена необходимостью подготовки специалистов, способных работать на стыке сетевой эксплуатации и кибербезопасности. В условиях, когда граница между «сбоем софта» и «взломом системы» размыта, понимание принципов анализа цифровых следов становится базовой инженерной компетенцией.

* АНАЛИЗ ЦИФРОВЫХ ИНЦИДЕНТОВ: ЗАДАЧИ ИНЖЕНЕРА

Цифровая криминалистика в телекоме — это метод анализа состояний сложных систем. Инженер работает с последствиями: аномалиями трафика, отказами узлов агрегации, нарушениями целостности баз данных. Криминалистический подход превращает разрозненные логи в связную историю инцидента.

Фиксация состояния: от образов к Triage-анализу

Анализ всегда начинается с фиксации «снимка» системы. В классическом инженерном сценарии используются инструменты побайтового копирования: FTK Imager в Windows или dd, dc3dd, Guymager в Linux. Однако в телеком-инфраструктуре создание образа сервера на десятки терабайт часто невозможно из-за требований к доступности (SLA).
В таких случаях применяется тактика Triage (экспресс-сбор). Вместо полного образа инженер фиксирует «летучие данные» (volatile data): таблицы маршрутизации, активные сетевые сессии, содержимое кэша и списки запущенных процессов. Это позволяет сохранить состояние системы до того, как фоновые процессы или перезагрузка исказят картину. Для этого используются специализированные скрипты и утилиты сбора артефактов, гарантирующие минимальное влияние на исследуемую среду.
Анализ удаленных данных и восстановление событий
Восстановление данных используется инженером для выявления следов несанкционированных изменений. Удалённые конфигурационные файлы или стертые журналы — явный маркер попытки скрыть причины сбоя. В Windows-среде применяются R-Studio, Recuva, в Linux — TestDisk, Foremost, Scalpel. Для инженера связи это способ отличить случайный сбой файловой системы от преднамеренной очистки логов.
Файловая система и хронология
Файловая система — это летопись работы узла. Анализ временных меток доступа и изменения файлов (MAC-timestamps) через Autopsy или The Sleuth Kit позволяет восстановить последовательность действий персонала или скриптов. В телекоме это критично для анализа серверов биллинга, систем мониторинга и контроллеров SDN-сетей.
Оперативная память (RAM) как источник истины
Оперативная память содержит данные, которые никогда не попадают на диск: ключи шифрования, открытые сокеты, запущенные в памяти вредоносные модули. Для фиксации ОЗУ применяются DumpIt, WinPMEM (Windows) или LiME, AVML (Linux). Для инженера это единственный способ проанализировать инцидент «в моменте», когда система еще активна, но уже ведет себя аномально.
Сетевой трафик и телеком-протоколы
Трафик — главный носитель информации в связи. Инженерный анализ выходит за рамки просмотра HTTP-пакетов. Важнейшее значение имеет исследование дампов на уровне протоколов маршрутизации (BGP, OSPF) и сигнализации (SIP, Diameter). Помимо Wireshark и tcpdump, используются данные NetFlow/IPFIX, извлекаемые с интерфейсов маршрутизаторов. Сеть рассматривается как модель поведения, где любая аномалия в задержках или направлениях потоков является следом инцидента.
Логи оборудования и журналы аутентификации
Логи формируют временной скелет анализа. Помимо системных журналов ОС (анализируемых через Event Log Explorer или стек ELK/OpenSearch), инженер связи опирается на журналы аутентификации оборудования (RADIUS/TACACS+). Сопоставление команд, введенных в консоль коммутатора, с временными метками деградации сервиса — базовый метод выявления человеческого фактора или

внутреннего нарушителя.

Встроенные устройства и прошивки (Firmware)

Узлы связи — это на 90% встроенные системы. Анализ прошивок с помощью Binwalk и Firmware-Mod-Kit позволяет проверить целостность ПО вендора. Инструменты типа Ghidra или Radare2 используются для анализа бинарного кода, если есть подозрение на наличие недокументированных возможностей (бэкдоров), влияющих на устойчивость инфраструктуры.

Искусственный интеллект как аналитический фильтр

Инструменты ИИ (OpenCV, TensorFlow, scikit-learn) в инженерном анализе играют роль фильтра, способного обработать гигабайты логов или терабайты трафика. Они ускоряют поиск аномалий, классифицируют типы сетевых атак и помогают в анализе аудио/видео данных. Инженер должен помнить: ИИ — это инструмент автоматизации внимания, но финальное решение и интерпретация всегда остаются за специалистом.

* УЧЕБНО-ПРАКТИЧЕСКИЙ МОДУЛЬ

В основной статье были рассмотрены классы инструментов цифровой криминалистики, инженерного анализа и расследования инцидентов. Однако простое перечисление средств не отвечает на вопрос: как именно специалист использует их в реальной работе. Учебный блок предназначен для демонстрации единого цикла, где инструменты применяются как элементы одной процедуры. Такой подход характерен для инженеров связи, системных администраторов и специалистов по эксплуатации, где требуется восстановление фактической картины событий.

Учебный модуль: практический цикл анализа инцидента в инфраструктуре

Исходная инженерно-криминалистическая ситуация

На рабочем узле (компьютере, сервере или маршрутизаторе) зафиксированы признаки аномалии: исчезновение данных, нестабильность сессий, подозрительная сетевая активность. Прямая проверка системы «на месте» недопустима, так как любые действия изменят состояние данных. Цель — понять, что произошло, в какой последовательности и с какими последствиями.

Этап 1. Фиксация состояния системы как отправная точка

Работа начинается с создания побайтовой копии (FTK Imager, dd, Guymager). В условиях корпоративной сети и работающих сервисов применяется тактика Triage — быстрый сбор летучих данных (процессы, сетевые порты, ARP-таблицы).

* Роль ИИ: Первичная классификация процессов на этапе сбора для выделения подозрительных узлов, требующих немедленного дампирования.

Этап 2. Первичный обзор структуры данных и ориентирование

Образ монтируется в режиме «только чтение» через OSFMount. В Autopsy специалист изучает профили пользователей, конфигурации (/etc/ или реестр Windows) и временные папки.

Аналитическое значение: Формируется карта исследования, исключающая хаотичный поиск.

Этап 3. Анализ удалённых данных как индикатор вмешательства
Использование PhotoRec или Scalpel для поиска удаленных журналов (логов) и конфигураций. В локальных сетях администратор также анализирует теневые копии (VSS). Факт и характер удаления — ключевой элемент реконструкции событий.
Этап 4. Построение временной линии событий (Timeline)
Агрегация данных из логов ОС, журналов контроллеров домена и сетевого оборудования через Plaso и Timesketch.
* Роль ИИ: Кластеризация миллионов строк логов с помощью NLP-моделей для выделения уникальных цепочек событий (например, подозрительный вход -> повышение привилегий -> сетевой шторм).
Этап 5. Анализ сетевой активности (в ЛВС и глобальных сетях)
Анализ дампов в Wireshark и NetworkMiner. Поиск признаков горизонтального перемещения (Lateral Movement) внутри ЛВС или аномалий в протоколах маршрутизации (BGP, OSPF).
* Роль ИИ: Автоматическое выявление отклонений от «базовой линии» (Baseline) типичного сетевого поведения узла.
Этап 6. Работа «на горячую» и Big Data (Расширенный анализ)
При невозможности остановки критического узла применяется Live Response (Velociraptor, eBPF/Tetragon) для мониторинга действий в реальном времени. Для анализа терабайтов данных NetFlow и системных событий используется стек ClickHouse + Grafana. Это позволяет находить скрытые угрозы, растянутые во времени.
Этап 7. Формирование аналитического заключения
Синтез результатов: описание состояния системы, последовательность отклонений и инженерно-аналитическое описание фактов для принятия технических и правовых решений.
Учебная практика. Модуль 2: Анализ мобильных устройств и терминалов
Мобильное устройство часто выступает инструментом удаленного администрирования или каналом утечки.
* Методы: Логическое извлечение (ADB, libimobiledevice) или физическое (Root/Jailbreak).
* Роль ИИ: Использование компьютерного зрения для поиска на скриншотах паролей, QR-кодов и схем инфраструктуры.
* Корреляция: Сопоставление активности мобильных SSH-клиентов и мессенджеров с логами доступа к корпоративным ресурсам.
Учебная практика. Модуль 3: Типовые ошибки анализа
* Анализ без фиксации: Прямое вмешательство уничтожает временные метки.
* «Слоновья походка»: Массовый забор данных, парализующий работу корпоративной сети.
* Доверие взломанным утилитам: Использование системных команд на скомпрометированном узле вместо доверенных статических бинарников.
* Избыточная вера в ИИ: Автоматическая классификация — лишь помощник, финальное решение всегда за специалистом.

Учебный модуль: Анализ виртуализированных сред и облачной инфраструктуры (SDN/NFV)
В условиях современной инфраструктуры связи большинство сервисов развернуты в виртуальной среде (KVM, VMware) или контейнерах (Docker, Kubernetes). Инциденты здесь требуют специфических методов извлечения артефактов, так как физический доступ к нодам часто ограничен.
Методы и инструменты работы:
 * Захват состояния ВМ (Snapshot Forensics): Использование снимков оперативной памяти (.vmem) и дисков (.vmdk, .qcow2) виртуальных машин. Это позволяет проводить анализ без остановки соседних сервисов на гипервизоре.
 * Анализ виртуальных коммутаторов: Изучение потоков данных внутри Open vSwitch (OVS) или vSphere Distributed Switch. Настройка Port Mirroring (SPAN/ERSPAN) на виртуальном уровне для перехвата межконтейнерного трафика (East-West traffic).
 * Контейнерная форензика: Использование инструментов Runtime Security (Falco, Inspektor Gadget) для отслеживания аномальных системных вызовов внутри подов. Ручной анализ манифестов и логов управления (Kubernetes Audit Logs).
УЧЕБНЫЕ КЕЙСЫ (ИНЖЕНЕРНЫЙ АНАЛИЗ)
Кейс 1. «Деградация BGP-связности и подмена AS-Path»
Ситуация: Зафиксировано аномальное изменение маршрутов к критическому сегменту сети. Трафик перенаправлен через транзитную автономную систему с сомнительной репутацией.
Требуется: Выполнить ручной разбор дампов BGP-обновлений (MRT-формат). Проверить атрибуты AS_PATH, NEXT_HOP и COMMUNITY. Провести верификацию префиксов по базам данных RPKI и IRR. Идентифицировать узел, инициировавший нелегитимный анонс.
Кейс 2. «Аномалии в стеке виртуализированных станций (vBS) и Open RAN»
Ситуация: Наблюдается рассинхронизация интерфейсов Fronthaul (на базе eCPRI) и рост задержек в радиоканале. Подозрение на компрометацию гипервизора или среды управления.
Требуется: Анализ конфигурационных файлов YAML и Docker-манифестов. Ручная инспекция системных вызовов через strace и анализ сетевых пространств имен (netns) для выявления скрытых туннелей внутри виртуальной инфраструктуры.
Кейс 3. «Компрометация SDN-контроллера и подмена правил потоков»
Ситуация: Трафик внутри ЦОД самопроизвольно перенаправляется на неавторизованный узел-анализатор, минуя системы защиты.
Требуется: Снятие дампа памяти процесса SDN-контроллера. Анализ текущей таблицы потоков (Flow Table) через команды управления контроллером. Поиск несанкционированных API-запросов в логах управления облачной платформой.
Кейс 4. «Анализ гибридной DDoS-атаки методами Big Data»
Ситуация: Пограничный маршрутизатор находится под воздействием комбинированного флуда.

Механизмы автоматической защиты не справляются с динамически меняющимися заголовками пакетов.
Требуется: Формирование SQL-запросов к СУБД ClickHouse для агрегации NetFlow-данных по специфическим флагам. Ручное создание ACL-списков на основе выявленных закономерностей распределения трафика (Entropy analysis).
Кейс 5. «Форензика мобильного терминала администратора»
Ситуация: С учетной записи администратора внесены деструктивные изменения в конфигурацию ядра сети в нерабочее время.
Требуется: Извлечение файловой системы мобильного устройства. Анализ SQLite-баз мессенджеров и журналов SSH-клиентов. Сопоставление временных меток в логах смартфона с журналом команд на сетевом оборудовании.
Кейс 6. «Скрытая эксфильтрация данных через DNS-туннелирование»
Ситуация: Обнаружена утечка информации, маскирующаяся под легитимные DNS-запросы к внешним резолверам.
Требуется: Сбор и ручной анализ дампов трафика (pcap). Декодирование полезной нагрузки из полей TXT или AAAA записей. Восстановление переданных файлов из фрагментированных пакетов и идентификация командного центра (C2).
Кейс 7. «Манипуляция сигнализацией в сетях 4G/5G (SS7/Diameter)»
Ситуация: Зафиксированы случаи нелегитимной перерегистрации абонентов и перехвата входящих вызовов.
Требуется: Анализ протоколов MAP/TCAP и Diameter. Ручное отслеживание цепочек сигнальных сообщений для поиска точки инъекции ложных ответов HLR/HSS. Верификация глобальных заголовков (Global Titles).

ЗАКЛЮЧЕНИЕ

Современная архитектура сетей связи и корпоративных ИТ-инфраструктур к 2026 году достигла критического уровня сложности, при котором традиционные методы мониторинга и разграничения доступа уже не способны гарантировать устойчивость систем. Цифровая криминалистика и инженерный анализ инцидентов сегодня трансформировались из вспомогательных инструментов в фундаментальную основу обеспечения живучести сетей. Проведенный обзор методологий и практических кейсов наглядно демонстрирует, что расследование любого инцидента — от локального сбоя до целенаправленной атаки на ядро сети — требует от инженера синтетического мышления, объединяющего навыки системного администрирования, глубокого знания стека протоколов (L2–L7) и методов работы с большими данными.
Ключевой вывод представленного исследования заключается в том, что в условиях тотальной виртуализации (NFV) и программно-определяемых сетей (SDN) понятие «цифрового следа»

кардинально изменилось. Артефакты теперь распределены между физическими носителями, оперативной памятью гипервизоров и эфемерными контейнерами. Это диктует необходимость внедрения процедур Live Response и Triage как стандарта операционной деятельности. Инженер не может позволить себе ожидание полной остановки систем; он должен уметь извлекать достоверные данные «на лету», используя инструменты eBPF, зеркалирование трафика внутри виртуальных коммутаторов и моментальные снимки состояний оперативной памяти. Без этих навыков расследование инцидентов в облачных средах и сетях 5G становится невозможным, так как улики уничтожаются вместе с перезапуском скомпрометированного микросервиса.

Особое внимание в работе уделено инструментарию Big Data и системам машинного обучения. Важно понимать, что в сетях с терабитными скоростями ручной анализ дампов трафика (pcap) применим лишь для точечной верификации гипотез. Масштабное детектирование таких угроз, как скрытая эксфильтрация данных (Exfiltration) или аномалии в протоколах сигнализации (SS7/Diameter/HTTP2), требует использования аналитических платформ сверхвысокой производительности, таких как ClickHouse или OpenSearch. Внедрение ИИ в этот процесс — не дань моде, а жесткая технологическая необходимость. Алгоритмы кластеризации и рекуррентные нейронные сети позволяют «схлопывать» миллиарды логов в единые цепочки событий, подсвечивая те паттерны, которые объективно недоступны человеческому восприятию из-за их распределенности во времени и пространстве. Однако финальная интерпретация и принятие решения остаются за инженером, чья интуиция базируется на фундаментальном понимании работы систем (от теории массового обслуживания до кибернетики).

Инженерно-философский аспект данной работы также подчеркивает значимость использования Open Source решений. В условиях глобальной нестабильности и закрытости проприетарных технологий, прозрачность инструментов анализа (таких как Wireshark, Autopsy, Velociraptor) становится единственной гарантией того, что методы расследования сами не содержат скрытых уязвимостей. Возможность верифицировать код инструментария и адаптировать его под специфику конкретного телеком-узла или ЦОДа является залогом технологического суверенитета и информационной безопасности. Системная методология, описанная в модулях учебной практики, призвана структурировать хаотичный процесс поиска «виновного» в строгий алгоритм доказательного исследования, результаты которого могут быть использованы не только для технической коррекции сети, но и в рамках правового поля.

В заключение стоит отметить, что типовые кейсы, разобранные в модуле — от BGP Hijacking до форензики мобильных терминалов администраторов — показывают: самым слабым звеном остается человеческий фактор и интерфейс взаимодействия человека с машиной. Никакая система защиты не будет эффективной, если инженер не понимает логику «цифрового почерка» злоумышленника или не умеет отличить аппаратный сбой от квалифицированного вмешательства в таблицу потоков SDN-контроллера. Подготовка специалистов нового поколения, способных работать на стыке фундаментальной науки, практического программирования и криминалистики — это единственный

путь к созданию защищенного цифрового будущего. Представленный материал служит базисом для формирования таких компетенций, переводя инженерный состав от пассивного наблюдения к активному противодействию и глубокому анализу инфраструктурных рисков. Системный подход, внимание к деталям и владение передовым стеком технологий — вот три столпа, на которых должна строиться современная служба эксплуатации и безопасности любых масштабируемых сетей.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ И ИСТОЧНИКОВ

* Autopsy Cloud and Network Forensics. Справочное руководство пользователя системы анализа цифровых доказательств.
* Wireshark Network Analyzer. Техническая спецификация и руководство по анализу протоколов L2-L7.
* Velociraptor Endpoint Management. Инструкция по развертыванию систем Live Response и сбору Triage-артефактов.
* FTK Imager & Guymager. Методология создания побайтовых копий носителей и дампов оперативной памяти.
* Plaso & Log2Timeline. Руководство по автоматизированной агрегации и парсингу системных журналов событий.
* Timesketch & Grafana. Сборник методик по визуализации временных линий инцидентов и сетевой телеметрии.
* ClickHouse Analytical Stack. Документация по построению высоконагруженных систем хранения NetFlow и IPFIX данных.
* Falco & Tetragon Runtime Security. Руководство по мониторингу системных вызовов в контейнеризированных средах Kubernetes.
* NetworkMiner & PhotoRec. Инструкции по пассивному анализу сетевого трафика и восстановлению фрагментированных данных.
* OSFMount & Mount-Image-Pro. Методические указания по монтированию криминалистических образов в режиме Write-Protect.
* MITRE ATT&CK Framework. Справочник техник и тактик противодействия атакам на сетевую и облачную инфраструктуру.
* OWASP Network Security Project. Открытые исследования уязвимостей сетевых протоколов и методов их эксплуатации.
* SANS Digital Forensics and Incident Response (DFIR). Сборник плакатов и чек-листов по анализу сетевых вторжений.
* Bellingcat OSINT Investigation Techniques. Руководство по поиску и верификации данных из открытых источников в инфраструктурных исследованиях.
* Project Zero (Google). Исследования уязвимостей «нулевого дня» в ядрах операционных систем и сетевых стеках.

* Davidoff, S. Network Forensics: Tracking Hackers through Cyberspace / S. Davidoff, J. Ham. – Upper Saddle River : Prentice Hall, 2024. – 544 p.
* Тощук, С. Н. Форензика в системах IIoT и 5G-сетях: практическое руководство / С. Н. Тощук. – Алматы : Техносфера, 2025. – 312 с.
* Андреев, А. В. Противодействие преступлениям в сфере информационных технологий : учебник / А. В. Андреев, Д. В. Галиев. – Алматы : ИНФРА-М, 2025. – 450 с.
* Gregg, B. BPF Performance Tools: Deep Visibility into Software and Systems / B. Gregg. – New Jersey : Addison-Wesley, 2024. – 880 p.
* Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet / E. Casey. – London : Academic Press, 2024. – 720 p.